---Information Technology (IT) Specialist (GS-2210)
IT Security Competency Model---

TECHNICAL COMPETENCIES

Competency	*Definition*
Computer Forensics	Knowledge of tools and techniques pertaining to legal evidence used in the analysis of information contained within and created with computer systems and computing devices.
Example Behaviors by Proficiency Level	
Level 1 (Basic)	• Understands basic concepts of the full life cycle of forensic investigation and analysis, including acquiring and performing analysis of electronic data for legal evidence and recovering data in the event of a hardware or software failure.
Level 2 (Foundational)	• Assists in the use of computer forensic tools and techniques for data analysis; describes basic concepts behind chain of custody of digital evidence, and preservation of legal evidence.
Level 3 (Intermediate)	• Possesses extensive knowledge of computer forensics tools and techniques. • Acquires, analyzes and reports findings of forensic evidence.
Level 4 (Advanced)	• Monitors industry trends and marketplace experiences for impact on organization. • Defines and implements strategies for contingency and disaster recovery, preservation of electronic evidence, data recovery and continuity of operations plans for information systems. • Performs multiple, complex forensic examinations.
Level 5 (Expert)	• Coordinates with other Federal, state, local and private sector law enforcement and other computer forensic entities to resolve issues. • Coordinates and builds internal and external consensus for organizational computer forensics program. • Performs computer forensics at the expert level (e.g., reverse engineering Malware).

Competency	*Definition*
Configuration Management	Knowledge of the principles and methods for control of changes made to information systems components throughout the information system life cycle.
Example Behaviors by Proficiency Level	
Level 1 (Basic)	• Implements configuration management as a component of CMMI for large systems. • Identifies control items.
Level 2 (Foundational)	• Implements configuration management as a component of CMMI for large systems. • Identifies control items.

Level 3 (Intermediate)	• Implements configuration management as a component of CMMI for large systems. • Identifies control items.
Level 4 (Advanced)	• Implements configuration management as a component of CMMI for large systems. • Identifies control items.
Level 5 (Expert)	• Intimately understands relationships between many different facets of configuration management. • Understands risk. • Implements configuration management as a component of CMMI for large systems. • Identifies control items.

Competency	*Definition*
Data Management	Knowledge of the principles, procedures, and tools of data management, such as modeling techniques, data backup, data recovery, data dictionaries, data warehousing, data mining, data disposal, and data standardization processes.
Example Behaviors by Proficiency Level	
Level 1 (Basic)	• Awareness of the basic concepts of data management.
Level 2 (Foundational)	• Basic understanding of data management principles, procedures and tools.
Level 3 (Intermediate)	• Interprets and applies concepts of data management principles, procedures and tools at a system level.
Level 4 (Advanced)	• Advanced understanding of data management principles, procedures and tools at an enterprise level.
Level 5 (Expert)	• Consults with, advises, and teaches others on data management. • Develops data management models. • Performs data management functions at multiple levels, including outside of the agency.

Competency	*Definition*
Encryption	Knowledge of procedures, tools, and applications used to keep data or information secure, including public key infrastructure, point-to-point encryption, and smart cards.
Example Behaviors by Proficiency Level	
Level 1 (Basic)	• Understands basic concepts of encryption technology. • Understand potential and existing algorithms. • Understands difference between symmetric and asymmetric encryption methodologies. • Implements or supports at least one type of encryption technology; identifies different types of encryption methods and associated technologies.
Level 2 (Foundational)	• Applies basic understanding of encryption principles, procedures and tools with supervision.
Level 3 (Intermediate)	• Uses knowledge of encryption principles and techniques (for

	example, PKI, symmetric and asymmetric key) for application, integration, and routine administration of the organizational security program. • Applies relevant cryptographic/encryption standards, products and protocols (for example, digital signatures, VPNs, smart cards, IPSEC, Secure Sockets Layer (SSL)) to operational situations.
Level 4 (Advanced)	• Integrates encryption into multiple applications and technologies. • Designs, supports and integrates encryption techniques across multiple platforms. • Analyzes correctness of a developer's implementation
Level 5 (Expert)	• Monitors new technologies, trends, and regulatory issues for impact on the enterprise-wide encryption program. • Analyzes, defines, develops, and implements enterprise-wide encryption strategies. • Consults with others to develop new encryption algorithms. • Analyze others' cryptography schemes.

Competency	***Definition***
Information Assurance	Knowledge of methods and procedures to protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.
Example Behaviors by Proficiency Level	
Level 1 (Basic)	• Familiar with the coordination of routine activities relating to information assurance. • Understands basic concepts of information assurance. • Analyzes and applies risk management principles to information systems.
Level 2 (Foundational)	• Describes basic information assurance concepts and vulnerabilities in applying technology to secure organizational systems and data. • Complies with information assurance standards, practices and procedures to perform routine operations.
Level 3 (Intermediate)	• Understands and applies knowledge of information assurance concepts (for example, firewalls, PKI, systems certification and accreditation, security vulnerability testing, SSL, IPSEC, VPNs) and their impact on the organization. • Tracks audit findings to recommend changes to information assurance standards and procedures.
Level 4 (Advanced)	• Implements and supports security software and hardware across multiple platforms, applications and architectures. • Develops and administers policies, procedures and standards to ensure desired levels of enterprise-wide information assurance.
Level 5 (Expert)	• Coordinates and builds consensus internal and external to the organization for the integration and implementation of information assurance strategies. • Establishes audit policy and reporting mechanisms for ensuring compliance with the information assurance standards.

Competency	***Definition***
Information Resources Strategy and Planning	Knowledge of the principles, methods, and techniques of information technology (IT) assessment, planning, management, monitoring, and evaluation, such as IT baseline assessment, interagency functional analysis, contingency planning, and disaster recovery.
Example Behaviors by Proficiency Level	
Level 1 (Basic)	• Organizes work according to established project strategies. • Assesses own work products and monitors progress against assigned goals. • Coordinates work with other employees on the project team. • Provides input on status of assignments.
Level 2 (Foundational)	• Participates in establishing deadlines for work/projects. • Establishes personal IT work priorities of a repetitive nature to meet individual work deadlines.
Level 3 (Intermediate)	• Establishes project requirements and priorities and develops strategies, including coordinating work requirements and project resources, to achieve short or long-term goals. • Monitors and evaluates project activities and outcomes. • Coordinates work with employees involved in other projects in the work unit. • Plans IT project requirements, such as identifying skills needed, determining assignments, establishing priorities and resource requirements. • Monitors and evaluates progress of work group to ensure that programs and policies are being implemented and adjusted as necessary to accomplish IT goals and time frames.
Level 4 (Advanced)	• Develops an organizational IT plan that meets the organization’s current mission and goals. • Develops plans and evaluation criteria to assess the effectiveness and adequacy of IT systems, which serve the needs of a large field office or organization.
Level 5 (Expert)	• Establishes organization/work unit needs and priorities and develops strategies to achieve multiple short-and long-term goals, including directing and monitoring work, and determining and allocating resources. • Monitors and evaluates organization/work unit performance. • Coordinates work activities with other organizations or parts of the organization. • Coordinates and monitors new IT projects with employees within and outside the office, with varying degrees of expertise by identifying work assignments, unit goals, and timeframes.

Competency	***Definition***

Information Systems Security Certification	Knowledge of the principles, methods, and tools for evaluating information systems security features against a set of specified security requirements.
Example Behaviors by Proficiency Level	
Level 1 (Basic)	• Describes basic concepts behind information systems security certification.
Level 2 (Foundational)	• Identifies phases and tasks involved in evaluating information systems security certification. • Understands the rationale behind, and the application of, security certification principles, methods (for example, risk assessment, systems security plan, disaster recovery plan) and tools to participate in the certification process.
Level 3 (Intermediate)	• Participates in the evaluation of information systems to develop certification and accreditation plans. • Applies appropriate security documentation in the development of the certification documentation (for example, risk assessment, systems security plan, disaster recovery plan).
Level 4 (Advanced)	• Evaluates information systems to identify residual risks to make recommendations to meet the appropriate organizational security requirements. • Ensures system requirements identified in the certification plan are incorporated into the systems development life cycle process. • Performs oversight of testing team activities.
Level 5 (Expert)	• Develops procedures and policies for certification and accreditation plans for information systems throughout the organization. • Ensures consistency across the organization for information systems security certification. • Performs certification testing against a wide variety of solutions (operating systems, databases). • Understands application of control frameworks against particular technologies. • Performs penetration testing.

Competency	*Definition*
IT Security Architecture	Knowledge of architectural methodologies used in the design and development of information systems, including the physical structure of a system's internal operations and interactions with other systems and k knowledge of standards that either are compliant with or derived from established standards or guidelines.
Example Behaviors by Proficiency Level	
Level 1 (Basic)	• Describes the major components of IT security architecture. • Identifies local hardware, software and telecommunications components. • Follows policies, standards, and procedures. • Obtains documentation and information on the IT security

	standards and their uses.
Level 2 (Foundational)	• Interprets and uses IT security architectural guidelines. • Describes IT security architectural initiatives and specifications for own area. • Describes technical standards and procedures that affect own area. • Interprets policy and standards documentation.
Level 3 (Intermediate)	• Integrates and migrates existing and planned platforms. • Identifies IT security architecture issues and considerations for applicability and risk. • Applies standards and procedures relevant to own function on own initiative. • Contributes to the development and implementation of organization standards.
Level 4 (Advanced)	• Designs operating platforms for multiple functions. • Assesses vendor and industry experience to determine the impact on the organization. • Collaborates with other functions on establishing and documenting joint standards. • Uses existing and evolving technology standards to improve the consistency of organization's IT efforts.
Level 5 (Expert)	• Defines the organization's IT security architecture. • Leads in developing standards and procedures for a major functional area within the organization. • Manages organizational and functional adherence to standards as part of risk management and assessment. • Keeps abreast of emerging IT security architecture technologies and potential security implications. • Applies and builds into security architecture and incorporates in to as is and to be plans.

Competency	***Definition***
Network Security	Knowledge of methods, tools, and procedures, , to protect the organization's system boundaries and to prevent information systems vulnerabilities, and provide or restore security of information systems and network services.
Example Behaviors by Proficiency Level	
Level 1 (Basic)	• Describes basic security concepts behind information systems/ networks.
Level 2 (Foundational)	• Adheres to standards and procedures of information systems and network security. • Understands use of IPs, firewalls, VPNs, network access control, availability management.
Level 3 (Intermediate)	• Participates in the analysis, evaluation, development, coordination, and dissemination of security tools and procedures to eliminate system vulnerabilities. • Interprets and applies information systems/network security

	guidelines to ensure, protect and restore services and capabilities.
Level 4 (Advanced)	• Develops procedures and policies for evaluating, coordinating and disseminating security tools. • Defines and implements strategies for security planning and testing to eliminate information system vulnerabilities. • Applies network security on networks.
Level 5 (Expert)	• Coordinates and builds consensus across an organization for security planning and implementation. • Leads in the analysis, evaluation, development, coordination and dissemination of security tools and procedures to eliminate system vulnerabilities. • Independently applies network security on large scale (enterprise, department level) networks.

Competency	***Definition***
Physical Security	Use of information systems in support of physical security principles.
Example Behaviors by Proficiency Level	
Level 1 (Basic)	• Understands basic concepts of physical security.
Level 2 (Foundational)	• Identifies assets to determine value and criticality. • Assesses the nature of threats so the scope of the problem can be determined.
Level 3 (Intermediate)	• Performs a risk analysis so appropriate countermeasures can be developed.
Level 4 (Advanced)	• Develops systems and implement recommended solutions to solve identified physical security problems. • Implement procedures for ongoing monitoring and evaluation of physical security measures. • Identifies measures and components to match requirements of the solution or recommendation. • Outlines and documents recommendations with relevant reasons for presentation to a facility so that appropriate choices can be made.
Level 5 (Expert)	• Performs cost analysis of proposed integrated measures to ensure efficiency of implementation and operation.

Competency	***Definition***
Project Management	Knowledge of the principles, methods, or tools for developing, scheduling, coordinating, and managing projects and resources, including monitoring and inspecting costs, work, and contractor performance.
Example Behaviors by Proficiency Level	
Level 1 (Basic)	• Understands basic Project Management concepts.
Level 2 (Foundational)	• Assists lead project manager with day-to-day coordination and direction of team members.
Level 3 (Intermediate)	• Guides project personnel to achieve the established objectives.

	• Works in a matrix management environment to achieve project work.
Level 4 (Advanced)	• Applies complex budgets to track the status of project management resource usage. • Adjusts and maintains resource requirement estimates based upon project resource input updates.
Level 5 (Expert)	• Develops and presents briefings to executive audiences, including topics such as project status, project goals and objectives, and the project plan. • Acquires the appropriate resources and clarifies the roles and responsibilities of the project personnel.

Competency	***Definition***
Risk Management	Knowledge of methods and tools used for risk assessment and mitigation of risk.
Example Behaviors by Proficiency Level	
Level 1 (Basic)	• Understands the rationale behind the need for risk management.
Level 2 (Foundational)	• Identifies general phases and tasks involved in information systems risk assessments. • Understands basic concepts of methods and tools used for risk assessment as applied to information systems. • Assists in identification and mitigation of hardware/software risks and vulnerabilities for a specific area (for example, operating system, application level).
Level 3 (Intermediate)	• Participates in the analysis, evaluation, development, coordination, and dissemination of risk management methods and tools.
Level 4 (Advanced)	• Contributes to the development and implementation of specific risk management policies and procedures.
Level 5 (Expert)	• Defines and analyzes risk management, assessment, and mitigation procedures in accordance with organizational goals. • Directs and coordinates organization’s comprehensive risk management program, which encompasses cross-functional security disciplines (for example, technical, administrative, personnel, physical security). • Understands the differences between quantitative and qualitative risk assessments. • Understands and applies how other industries manage risk, tools and methodologies used to support risk-based decisions.

Competency	***Definition***
Software Security	Knowledge of the secure principles, methods, and tools used in the software development life cycle.
Example Behaviors by Proficiency Level	
Level 1 (Basic)	• Understands basic software security concepts such as the flaws that can exist in software.

	• Detects malicious code and develops code and routines that secure software from exploitation
Level 2 (Foundational)	• Runs and analyzes results provided by data tools.
Level 3 (Intermediate)	• Reviews and audits code to detect software flaws. • Remediates vulnerabilities.
Level 4 (Advanced)	• Understands relationship between different programming languages and their inherent vulnerabilities.
Level 5 (Expert)	• Audits potential software and architectures for broad ranges of vulnerabilities. • Develops mitigations. • Addresses software security in the life cycle. • Writes code to automatically exploit vulnerabilities in an automated fashion.

Competency	***Definition***
Systems Life Cycle	Knowledge of systems life cycle management concepts used to plan, develop, implement, operate, and maintain information systems.
Example Behaviors by Proficiency Level	
Level 1 (Basic)	• Applies awareness of basic models and methodologies of systems life cycle development. • Familiarity with at least one development methodology
Level 2 (Foundational)	• Familiarity with multiple development methodologies.
Level 3 (Intermediate)	• Interprets and applies concepts of at least one development methodology
Level 4 (Advanced)	• Interprets and applies concepts of multiple development methodologies.
Level 5 (Expert)	• Creates, applies, integrates and executes system development life cycle methodologies and models.

Competency	***Definition***
Systems Testing and Evaluation	Knowledge of the principles, methods, and tools for analyzing, developing and executing systems test and evaluation procedures and technical characteristics of IT systems, including identifying critical operational issues.
Example Behaviors by Proficiency Level	
Level 1 (Basic)	• Applies basic understanding of systems testing principles, methods and tools.
Level 2 (Foundational)	• Applies concepts related to systems testing principles, methods and tools. • Performs systems testing events at a component level.
Level 3 (Intermediate)	• Interprets and applies systems testing principles, methods and tools. • Performs repeated systems testing events at a systems level across multiple platforms and with an increasing complexity.
Level 4 (Advanced)	• Applies advanced understanding of systems testing principles,

	methods and tools. • Performs repeated systems testing events at an enterprise level across multiple platforms and with an increasing complexity.
Level 5 (Expert)	• Consults, advises, and teaches others in the application of systems testing principles, methods and tools. • Drafts a large number of test plans. • Applies tools in an automated fashion.

GENERAL COMPETENCIES

Competency	*Definition*
Interpersonal Skills	Shows understanding, friendliness, courtesy, tact, empathy, concern, and politeness to others; develops and maintains effective relationships with others; may include effectively dealing with individuals who are difficult, hostile, or distressed; relates well to people from varied backgrounds and different situations; is sensitive to cultural diversity, race, gender, disabilities, and other individual differences.
Example Behaviors by Proficiency Level	
Level 1 (Basic)	• Cooperates and works well with management, other employees, or customers during brief interactions. • Remains courteous when discussing information or eliciting non-sensitive or non-controversial information from people who are willing to give it. • Effectively handles situations involving little or no tension, discomfort, hostility, or distress; responds courteously to customer’s general inquiries. • Greets and assists visitors attending a meeting within own organization.
Level 2 (Foundational)	• Familiarizes new employees with administrative procedures and office systems.
Level 3 (Intermediate)	• Cooperates and works well with management, other employees, or customers, on short-term assignments. • Remains courteous when discussing information or eliciting moderately sensitive or controversial information from people who are hesitant to give it. • Effectively handles situations involving a moderate degree of tension or discomfort involving people who are demonstrating a moderate degree of hostility or distress. • Courteously and tactfully delivers effective instruction to frustrated customers. • Provides technical advice to customers and the security systems, data management procedures or analysis, software engineering, or web development. public on various types of IT such as

	communication or security systems, data management procedures or analysis, software engineering, or web development.
Level 4 (Advanced)	• Mediates disputes concerning system design/architecture, the nature and capacity of data management systems, system resources allocations, or other equally controversial/sensitive matters.
Level 5 (Expert)	• Establishes and maintains ongoing working relationships with management, other employees, internal or external stakeholders, or customers. • Remains courteous when discussing information or eliciting highly sensitive or controversial information from people who are reluctant to give it. • Effectively handles situations involving a high degree of tension or discomfort involving people who are demonstrating a high degree of hostility or distress. • Presents controversial findings tactfully to irate organization senior management officials regarding shortcomings of a newly installed computer system, software programs, and associated equipment.

Competency	***Definition***
Legal, Government and Jurisprudence	Knowledge of laws, legal codes, court procedures, precedents, legal practices and documents, Government regulations, executive orders, agency rules, Government organization and functions, and the democratic political process.
Example Behaviors by Proficiency Level	
Level 1 (Basic)	• Aware of Federal Information Security Management Act (FISMA) and Privacy Act, and other applicable IT security laws and policies. • Aware of the existence of National Institute of Standards and Technology (NIST) guidance in IT security.
Level 2 (Foundational)	• Understands the body of IT security guidance that exists for Federal Government agencies.
Level 3 (Intermediate)	• Interprets and applies the body of IT security guidance that exists for Federal Government agencies.
Level 4 (Advanced)	• Understands the body of IT security guidance that exists comprehensively across the Federal Government and equivalent international standards.
Level 5 (Expert)	• Contributes to the writing of IT security guidance and standards.

Competency	***Definition***
Problem Solving	Identifies problems; determines accuracy and relevance of information; uses sound judgment to generate and evaluate alternatives, and to make recommendations.
Example Behaviors by Proficiency Level	
Level 1 (Basic)	• Uses logic to identify alternatives to solve routine problems. • Reacts to and solves problems by gathering and applying information from standard materials or sources that provide a

	limited number of alternatives. • Investigates and employs assistance in resolving simple problems. • Collects needed information to outline a proposed solution to a simple problem.
Level 2 (Foundational)	• Takes action by contacting vendor concerning goods that arrived damaged.
Level 3 (Intermediate)	• Uses logic to identify alternatives to solve moderately difficult problems. • Identifies and solves problems by gathering and applying information from a variety of materials or sources that provide several alternatives. • Investigates, collaborates, and resolves computer problems of a moderate complexity. • Resolves computer equipment/software problems by researching and troubleshooting user manuals, Internet Web sites, talking with company technicians.
Level 4 (Advanced)	• Identifies areas of potential security vulnerabilities and generates alternatives to safeguard or to minimize those vulnerabilities. • Develops and proposes strategic alternate models to solve technological problems or requirements.
Level 5 (Expert)	• Uses logic to identify alternatives to solve complex or sensitive problems. • Anticipates problems, and identifies and evaluates potential sources of information and generates alternatives to solve problems where precedents do not exist. • Provides precedent-setting solutions to unique technical problems not previously encountered.

SKILLS

Skill	*Definition*
Continuity of Operations Planning	Building contingencies and strategies for minimizing financial and operational losses following service interruptions caused by natural, technological, and attack-related emergencies. Such planning includes the safety of employees, information, and services.
Network Configuration and Implementation	Programming of the layout and settings of the computers and equipment on an enterprise's local area network (LAN) or intranet. This includes devices like routers and gateways that interconnect the LAN with other LANs or the Internet.
Systems Security Applications	Activities related to the applications and tools that administrators use to manage various users, roles and groups to implement access and privilege controls for

	certain applications or against operating system resources.
Testing	Activities related to determining whether objectives are being met during hardware/software development. Testing can take place at a variety of levels such as the module, component, or system levels. Testing is also related to the various types of verification, validation and evaluation of whether or not a system satisfies its acceptance criteria. This process enables the customer to determine whether or not to accept the system.
UNIX Operating System	UNIX operating system that performs basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers. Unix is designed for use by many people at the same time (it is multi-user) and has TCP/IP built-in. UNIX is the most common operating system for servers on the Internet.
Wireless Technologies	Activities related to any technology that transmits information signals via radio waves rather than cables or wires, where individual units are connected to a network, such as cellular phones, networked laptops, and PDAs.